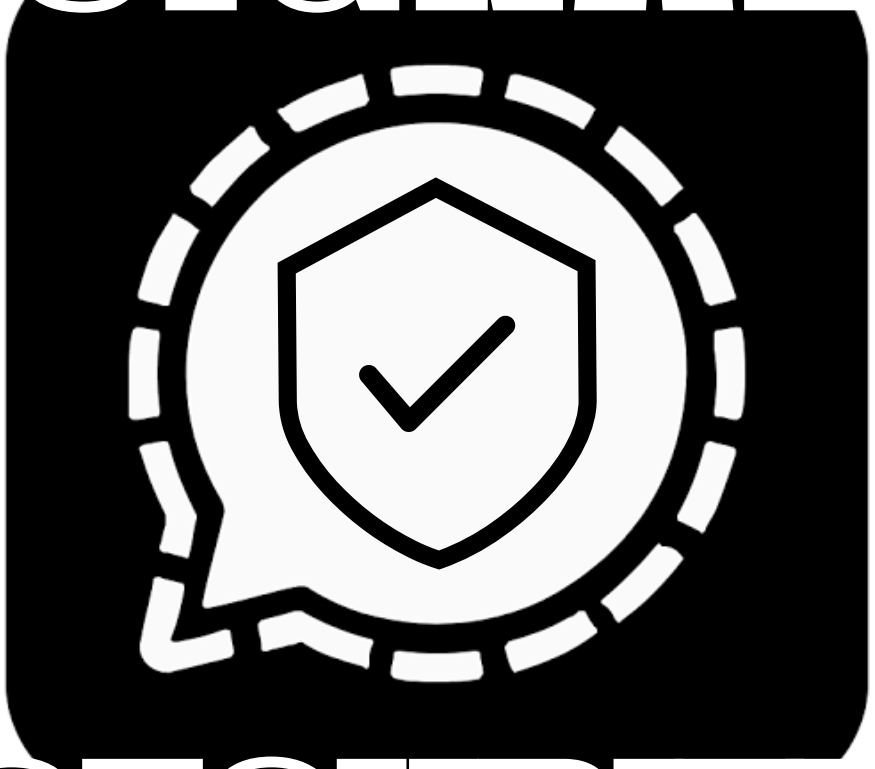
SIGNAL



SECURITY

WHAT IS IT & HOW TO DO IT

The Need For Privacy and Encryption

In a world of mass surveillance, privacy becomes all the more important no matter who you are or what you do.

Although not perfect, encryption is a great way to increase your personal security and protect your data. In very simplified terms, encryption is a bunch of complicated math equations that turn data and information from a digital standpoint into scrambled nonsense. Encrypted messages cannot be decrypted without a ‘key’ which is often built into phones, certain apps and programs.

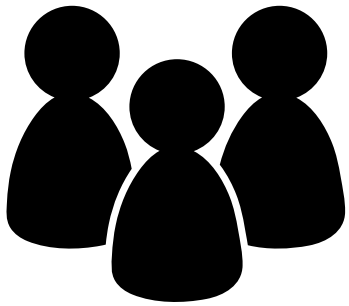
It doesn’t matter if you feel like you have nothing to hide when the State can at any time define what is wrong and right. The “wrong thing” could be about activities related to observing unlawful harassment and extrajudicial kidnapping at the hands of the state by the current administration and much more. Additionally, your lack of privacy and security can easily put others at risk, whether you know it or not.

There is a ton more reasons why security and privacy matters, but that’s not within the scope of this zine. We are going to be focusing on Signal as a more private and more secure means of communication. Check out some of the resources at the end for more information regarding security practices!

What is Signal?

Signal is a free, open-source, end-to-end encryption (E2EE) app that's been on the forefront of secure messaging apps. Signal requires a working phone number to use. E2EE is safest because only the sender and receiver have the "keys" to the encryption, not even Signal has the "keys"! Signals stores very little metadata, only the last day a user connected to the server and when the account was originally created.

Signal has been used in high security groups for a long time, from protesters to politicians, to people just looking for extra privacy when communicating. Keeping your messages private can also keep you out of legal trouble if you ever say what the government classifies as a "wrong thing".



It's best to assume that **nothing** online is secure. And while Signal is far more secure than other apps, *Signal is only as secure as you can make it.*

Protecting Your Identity

1. Do not use your full name in Signal, consider changing it to just your first name, your initials or a nickname.
    a. Change your name BEFORE you join a group chat, changing it in a group chat keeps that record and others can see changes made.
    b. Refer to each other using the name provided on the Signal chat, refrain from using people's real names when in a group chat where you don't know everyone or are engaging in higher risk activities.
2. Go to settings > Privacy > Phone number > Select "nobody" for who can see my phone number AND who can find me by my phone number.
3. To create a username people can find you with, go into Signal settings > Click on your profile name > Select username
    a. This is different from your profile name. It's not recommended to use your full name here either. This allows you to be searched via Signal without exposing your phone number.
4. Go to the settings in Signal > Account > Enable Registration Lock
    a. This prevents your phone number from being registered on a different device without the PIN you set up when you first register.
5. You can route your calls through Signal servers to hide your IP address by going to Signal settings > Privacy > Advanced and enanble 'Always Relay Calls'
    a. **IMPORTANT NOTE:** Enabling may reduce the call quality.

4

Protecting the Identity of Others

1. Go to settings > Chats > Turn off share contacts with iOS AND use contact photos
2. Go to settings > Privacy > Scroll down to ‘Calling’ and turn off “Show Calls in Recents“
3. Refer to each other using the name provided on the Signal chat, refrain from using people’s real names when in a group chat where you don’t know everyone or are in a group chat which is engaging in higher risk activities.
4. Leave and delete yourself from chats if you plan on travelling out of country or more than a few hours away, if you plan on partaking in risky actions, or aren’t able to keep up or engage with chats for awhile.
    a. If someone in a group chat doesn’t open messages for a while, even when other people have burned it, Signal stores that data. If the person who hasn’t opened messages for a while is compromised (ie: scam, arrest, etc), everyone’s information, data, and plans are then compromised.
5. If you know someone has been arrested or compromised that is also in Signal chats, notify an admin or the chat immediately so that the chat can be burned. More about burning chats on page 6!

5

Phone Settings for Signal

(using iOS/Apple settings- for non iOS, check resources page for more detailed instructions)

1. Go to phone settings (NOT Signal) > Apps > Signal > Make sure “contacts access” is set to none
2. Go to phone settings > Notifications > Scroll to select Signal > In Lock Screen Appearance, turn “Show Previews” to never
    a. Showing previews/reading notifications from lock or home screen decrypts the data immediately.
3. Go to phone settings > Apps > Signal > Apple Intelligence & Siri > Turn off “Learn from this App”
    a. *Some older phones or phones that haven’t been updated may not have this feature*.
4. Go to phone settings > General > Keyboards. Ensure that there are no keyboard apps downloaded or being used besides the default emoji and language choices. Keyboard apps often collect data even when not in use.
5. Disable AI notification summaries. Go to phone settings> Apple Intelligence & Siri > Toggle off “Apple Intelligence”
    a. *Some older phones or phones that haven’t been updated may not have this feature*.

6

Extra Security

1. Go to the settings in Signal > Privacy > Set Disappearing Messages to any time you want, as long as it's set.
2. Every few months or after any "risky" action is taken, "burn" a group chat so that any stored data between users is removed. This can be done by clicking into the group chat, then the header, scrolling to the bottom and clicking leave group. After you leave the group, ALSO delete the group by sliding the chat to the left to reveal a red delete button.
3. Turn off facial recognition/biometrics for your phone. **Always.**
4. Turn on Screen Hider when switching apps. Go into settings in Signal > Privacy > Enable "Hide Screen in App Switcher"
5. You can disable link previews as they are notorious for leaking data and adding tracking tokens simply by the image the preview generates. Go into settings in Signal > Chats > Disable "Generate Link Previews"
   a. If you are sending a link from Instagram or Facebook remove the tracking component by deleting the "?" in the link and everything after that... and the link still works! Do this even when 'Generate Link Previews' is disabled.
   b. Ex.--> everything bolded can be removed: https://www.instagram.com/p/DTlLGSggCRB/ **?igsh=eXo4eWN4cWRjd2E4**

7

General Rule of Thumb

1. Never screenshot a Signal chat. It becomes unencrypted and compromises yourself and others.
2. Leave and delete yourself from chats if you plan on travelling out of country or more than a few hours away, if you plan on partaking in risky actions, or aren't able to keep up or engage with chats for awhile.
3. Don't talk about anything illegal or that could get you arrested in Signal. Or anywhere online for that matter. If you must, a technology-free in person conversation is always safest.
4. NEVER use the desktop version of Signal. There is a loophole in the desktop version that stores data. Once you have downloaded and logged onto desktop Signal, that data and everyone who are in chats with you has been exposed and is now subject to tracking.
5. If someone you don't know texts or calls you, be cautious- you don't owe anyone a response.
6. Never tell anyone what your pin for Signal is.
7. Don't add people to a group chat without knowing who can/should be added. Also, don't ever add people you don't know. More on that on page 8!

8

Group Chats

Assume that there are always cops in chat **(which we don't want)** and that not everyone has the same security practices. Don't post anything you don't want read back to you in a court of law. Keep people on a need-to-know-basis.

If added to a group chat, check to see if there are any pinned comments or rules of the group. If you are unsure, you can message an admin to check chat rules and expectations, or directly ask the chat if appropriate. To ask an admin, click into the chat, then the chat header, scroll down to click see all members, and click on one of the contacts that says 'admin' behind their name, then message via chat.

Some questions that may be good to ask are: who is invited to the group, how are you asked to participate, how are decisions made, what kind of security is expected here, is this a post events only chat or is discussion allowed? If you're looking to add someone to a group chat, first make sure it's okay to do so. Second, it is **YOUR** job to onboard that person(s) with all the rules and security needed for the chat.

Group chats can cause lots of notifications so be mindful of posts and interactions (unless specified, you don't have to respond or thumbs up every message).

9

Signal Scams

Signal is safer not safe. Signal will never do the following:

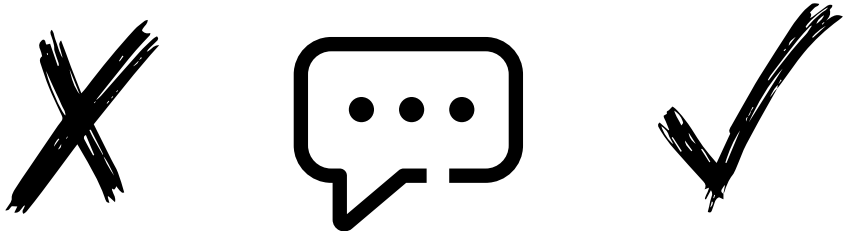
1. Signal will never initiate contact via in-app messages, phone calls, SMS, or social media. Signal ONLY communicates via their official email ONLY when you have reached out to them via the 'Contact Us' form in the Signal settings.

If anyone contacts you within Signal claiming to be a chat bot, security, support or representative from Signal, it is a SCAM. Immediately select Report and choose to Report and Block.

2. Signal will never ask for your verification code, recovery keys, or payment details. They may ask you to practice putting in your pin, but they will never ask for your code or pin via chat or any other form of communication.

3. Signal will never claim urgency. Ex: "Your account will be locked/lost unless...."

4. Signal will never ask you to set up 2-Factor Authentication.



10

Safety Numbers

Each Signal chat has a unique safety number that allows you to verify the security of your messages and calls with specific contacts. If a safety number has been marked as verified, any change must be manually approved before sending a new message.

Signal tells you when a safety number has changed. The most common scenarios where a safety number advisory is displayed are when a contact switches to a new phone or re-installs Signal, but these actions don't always result in a safety number change. However, if a safety number changes frequently or unexpectedly it may be a sign that something is wrong.

How do I view and verify safety number?
You must first accept the chat request, then open the chat and tap the header, select ‘View Safety Number’.

The easiest way to compare safety numbers is to scan your contact's QR code (ideally in person). You can also visually/audibly compare the numeric code. If the safety number is identical then you;re communicating with the right person. You can then tap "Mark as verified" to apply the setting on your side only, a checkmark will appear by their name.

It will remain verified unless the safety number changes or you manually change the verification status.

Sources/Other Resources

Some of these resources are quoted directly, some are just really good to check out!

How to download Signal and set it up:
https://ssd.eff.org/module/how-to-use-signal

Signal Security Checklist:
https://activistchecklist.org/signal/

Signal is Safer Not Safe Insta Graphic:
https://www.instagram.com/p/DURFEpPks-n/

No link, but the zine “What the Heck is Signal??”

Digital Security for Different Roles:
https://activistchecklist.org/

Mobile Phone Security:
https://www.sproutdistro.com/catalog/zines/security/mobile-phone-activists/

Digital Security for Activists:
https://files.sproutdistro.com/digital_security_for_activists-SCREEN.pdf

ICE Surveillance Info
https://www.eff.org/deeplinks/2026/01/ice-going-surveillance-shopping-spree

What is Security Culture:
https://www.sproutdistro.com/catalog/zines/security/what-is-security-culture-a-guide-to-staying-safe/#text

Assessing encryption messaging options:
https://crimethinc.com/2017/03/21/choosing-the-proper-tool-for-the-task-assessing-your-encryption-options

E2EE 101:
https://crimethinc.com/2017/03/08/end-to-end-encryption-101-what-does-e2ee-do-and-does-vault-7-mean-its-useless